Supplement to the Key Bridge Proposals to Administer an Environmental Sensing Capability

Response to FCC Request for Supplemental Information

GN Docket No. 15-319

Key Bridge Wireless LLC

Jesse Caulfield, CEO

1750 Tysons Blvd., Suite 1500
McLean, VA 22102

Phone: +1 (703) 542-4140

http://keybridgewireless.com

Document Information

Document Status	Public
Version	1.0.0
Date Printed	November 12, 2017
Copyright	© 2017 Key Bridge Wireless LLC. All Rights Reserved

Opening letter

Key Bridge Wireless LLC (fmr Key Bridge Global LLC, dba “Key Bridge”) is pleased to submit this additional supplement to our proposals to administer a Spectrum Access System (SAS) and a Environmental Sensing capability (ESC) in the 3.5 GHz frequency band.

This document is written to be directly responsive to the questions posed and, accordingly, makes reference to our separate *Proposal to Administer a Spectrum Access System* and to our *Proposal to Administer an Environmental Sensing Capability*.

We thank the Commission for this opportunity and are happy to provide any additional information the Commission may require to evaluate our proposals.

/s/

Jesse Caulfield, CEO
Key Bridge Wireless LLC

Proposal Supplement

The following sections supplement our *Proposal to Administer a Environmental Sensing Capability*.[1] A new Appendix 11 provides additional detail about our plans to implement radar detection and classification, technical specifications of ESC sensors, our ESC communications protocol and associated information and communication security strategies.

1 See Key Bridge *Proposal to Administer an Environmental Sensing Capability* (ESC Proposal), GN Docket 15-319, submitted March 15, 2016.

11 Appendix: ESC Sensor Node

Question: How will the ESC process sensor data? Please include information on sensor technology, frequency range, instantaneous bandwidth, technical description of the sensor, detection decision process, receiver sensitivity, received signal threshold, detection probability, and receiver resiliency to front-end saturations and burn-out. Please include a description of how the ESC will account for the impacts of nearby CBSDs on the system noise floor.

11.1 Technical description of the sensor

This section revises and extends Sec. 5.4 and replaces Sec. 6.7.[2]

The Key Bridge ESC sensor node is a two-component split system comprised of an outdoor receiver module and an indoor signal processing computer. The ESC outdoor unit is a solid-state, software defined system with no moving parts housed in an environmentally rugged IP67-rated weatherproof enclosure. The ESC indoor unit is a commercial off the shelf computer running a security enhanced embedded operating system with Key Bridge's proprietary spectrum signal processing and data reduction algorithms. The outdoor unit supports multiple antenna and is energized and controlled by a dedicated power over Ethernet communications link with the indoor unit. A typical configuration is shown below in Illustration 1.[3]

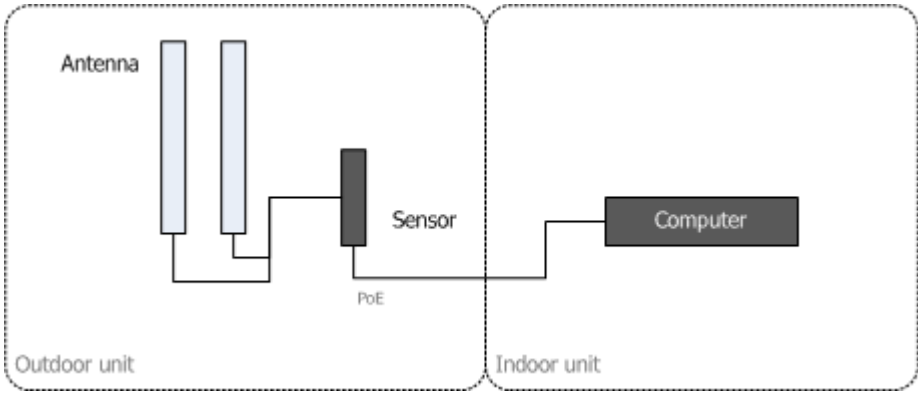

Illustration 1: The typical Key Bridge ESC sensor node inlcudes outdoor sensor and indoor computer subsystems.

2 Please note that Cognitive Systems Corp. is no longer a supplier or technology provider to Key Bridge.

3 In certain embodiments and installations the two subsystems may be combined in a single outdoor enclosure. This does not change the solution architecture. Up to four independent antenna are supported per sensor.

Key Bridge is presently evaluating several sensor products in our lab and in a private field trial to establish system capabilities and confirm end-to-end signal detection and classification performance. Here we provide typical sensor technology and technical specifications; the minimum technical specification that an ESC sensor node will exhibit.

Sensor technology	A solid state software defined receiver and vector signal analyzer providing real-time digital signal conversion and I/Q data stream generation.
Frequency range (sensor)	20 to 6,000 MHz
Instantaneous bandwidth	Varies by product. 20, 40 and100 MHz; may be extended with high-speed scanning
Receiver sensitivity	-110 dBm
Received signal threshold	-89 dBm/MHz[4]

4 Per NTIA/DoD specification.

11.2 Detection decision process

There are two primary frequency coordination systems In the 3.5GHz band: a Spectrum Access System (SAS), whose responsibility is to manage licensed and unlicensed users; and an Environmental Sensing Capability (ESC), whose function is to discern the presence (or absence) of a signal from an Incumbent User (IU) and to notify a SAS of the protection status of any effected Dynamic Protection Areas. A Dynamic Protection Area (DPA) is a predefined local protection area which may be activated or deactivated to protect a (federal) incumbent user. An activated DPA must be protected from aggregate CBSD interference.

For DPAs in coastal areas the Key Bridge ESC will be deployed and configured to provide incumbent protection based on a maximum allowable aggregate received power level from CBSDs to a prospective radar system of -144dBm/10MHz with a 95% reliability.[5]

Within an ESC service node each 10 MHz channel within a DPA geographic region may be either ACTIVE or INACTIVE according to the finite state diagram shown in Illustration 2.

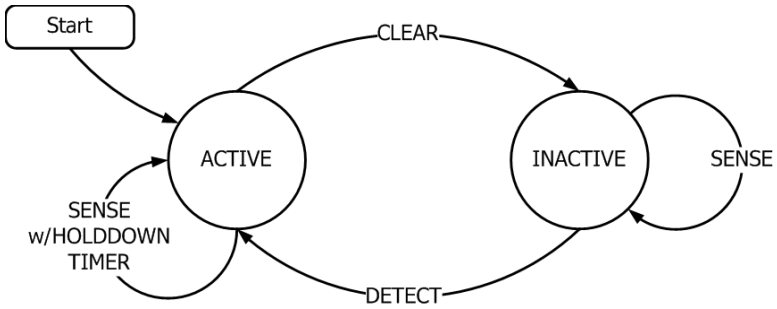

Illustration 2: DPA channel finite state machine.

When the ESC is initialized each DPA Channel ("DPAC") is placed into the ACTIVE state where the DPAC will remain until the ESC positively confirms that no IU is detected that affects the respective DPAC. If no IU is detected then the DPAC is immediately placed into the INACTIVE state, where it may remain indefinitely until an IU is detected.[6] If an IU is detected and determined to affect the DPAC the ESC changes the DPAC status to ACTIVE and initializes a HOLD-DOWN TIMER for that DPAC.[7] When the hold-down timer expires the ESC will review the status of the DPAC and adjust its state accordingly, either transitioning it to INACTIVE or resetting the hold-down timer.[8]

5 From Wireless Innovation Forum, *DPA Technical Requirements*. WINNF-17-I-00144 NTIA contributed June 19, 2017
6 A hold-down timer is not applied during the initialization phase.
7 The default hold-down timer is presently specified at two hours but may be adjusted or randomized to accommodate IU operational security requirements.
8 Hold-down timers are assigned on a one-to-one basis with each DPA + channel combination.

11.3 Receiver resiliency to saturation and burn-out

The ESC outdoor unit includes automatic control circuitry and programming logic with input attenuation of 60 dB (typ.) to minimize receiver saturation. Receiver automatic gain control response and recovery is near instantaneous.

The outdoor unit will include burnout protection capability in the form of a low barrier Schottky diode coaxial limiter installed in the antenna feed cables. The coaxial limiter is a passive solid state device with instantaneous protection up to 1,000W and recovery period of 1 second (typ.).

11.4 Operation in the presence of nearby CBSD

By industry agreement ESC sensor nodes may receive protection from CBSD aggregate interference up to the level specified for ESC certification.[9] If the local noise floor exceeds this power detection threshold the Key Bridge ESC may request interference protection from subscribing SASs. We do not believe this will be necessary except in rare circumstances. Under controlled lab tests the Key Bridge incumbent detection algorithms have successfully detected and classified very weak, P0N#1-type radar signals in the presence of TD-LTE and WiMAX-type carriers with high reliability.[10]

9 See Wireless Innovation Forum, *CBRS Operational and Functional Requirements*, R2-SGN-25: SAS ESC Sensor Protection, WINNF-TS-0112

10 P0N#1 is defined in Table 1 of NTIA Technical Memorandum 17-527 [DRAFT]. Our lab tests indicate greater than 95% probability of detection of P0N#1-type signals injected co-channel at 60 dB below a synthetic LTE and WiMAX carrier.

11.5 Incumbent Sensing and Detection

Question: What approach will the ESC employ (e.g., hardware upgrades, firmware updates) to detect new federal radar waveforms that may be deployed in the future? Please include the likely timeframe for implementation of these approaches.

In Section 6.4 we describe different strategies we anticipated for NIIU detection and identification. This has not changed. We are developing and propose to deploy and operate a conventional direct sensing solution using fixed infrastructure. We continue to research and in the future may proffer for test and evaluation an indirect sensing strategy should it prove feasible.

In Section 6.4.1 we describe basic incumbent signal characterization strategies. Referring again to Illustration 1 above the ESC sensor node indoor unit (computer) runs proprietary spectrum signal processing software against a continuous stream of data provided by the sensor node outdoor unit.

Key Bridge implements a set of signal feature extraction, decision tree analysis and machine learning algorithms for signal detection, classification and identification. We use a *Markov decision process* to detect and identify well behaved and well known signal types. Decision trees are flowchart like structures implemented in software to help choose between different outcomes and are widely used in in the analysis of complex data sets for medical diagnosis, cognitive science, artificial intelligence, program theory, engineering, and data mining. A Markov decision process is a type of decision tree that supports decision making (i.e. signal classification) against a data stream containing partly random and partly structured information. We use a *recurrent neural network* algorithm to detect and identify anomalous signal types that may be incompletely described.

Key Bridge will employ software application upgrades to the signal processing, feature extraction and detection algorithms running on the ESC indoor unit (computer) to detect new federal waveforms that may be deployed in the future.

Our signal detection and classification strategy relies upon extensive algorithm training against test and control data. In our experience identifying more ephemeral or imprecisely defined signals require more training time and test data. Assuming sufficient training data can be obtained our current best estimate is between three to nine months will be required to develop, train, evaluate and present for certification testing a new federal radar waveform detection capability.

11.6 ESC Concept of Operations

Question: How will the ESC determine and communicate the points or areas to be protected once radar operation is detected by the sensors? Please indicate if and how the solution aligns with any operational security requirements communicated by NTIA or DoD.

This extends Section 6 of our proposal.

All DPA regions and channels are actively protected in a SAS by default unless and until their absence is positively confirmed by a ESC, in accordance with Commission rules. The ESC, acting independently and autonomously to the SAS, notifies the SAS of the presence or absence of a federal IU by activating a DPA plus Channel combination ("DPAC").

Referring to Illustration 12, each ESC Sensor Nodes is deployed and configured to implement Rules-compliant radar signal detection and classification across a defined geographic region. Key Bridge will site and engineer each sensor node installation to provide maximum possible coverage of DoD/NTIA-defined DPA regions.

Referring to Illustration 13, positive (or negative) ESC signal detection and classification event information is conveyed from an ESC Sensor Node to the ESC Service Node that the Sensor Node is exclusively assigned to. ESC Sensor Nodes do not communicate or exchange information with other ESC Sensor Nodes in a peer-to-peer arrangement. Instead message routing is organized in a strictly hierarchical configuration where information is learned consolidated, obfuscated and then routed through a peering gateway to subscribing SASs using a proprietary Key Bridge peering protocol.

The Key Bridge ESC to SAS peering protocol includes strong counter party authentication, digital message signatures and encryption and conveys all the information necessary to conduct CBRS Rules compliant operation but no more.[11]

11 Key Bridge intends to include the ESC to SAS peering protocol with our ESC when the system is presented for formal evaluation and certification testing.

11.7 ESC Security Architecture

This extends Section 7 of our proposal.

The Key Bridge ESC enforces a *positive security model* to prevent unauthorized access, protect sensitive data and limit the effects of a potential breach, attach or failure. Referring to Illustration 29, the Key Bridge ESC Sensor Nodes will be deployed around certain inland areas and along the coast of the United States, its territories and assigns. Each ESC Service Node will control between five to seven Sensor Nodes depending upon local conditions, tower site availability and DPA coverage requirements.

Key Bridge earlier presented to DoD, and we summarize in Illustration 3 below, the learned information from each step in the IU detection and protection process with the Key Bridge ESC.

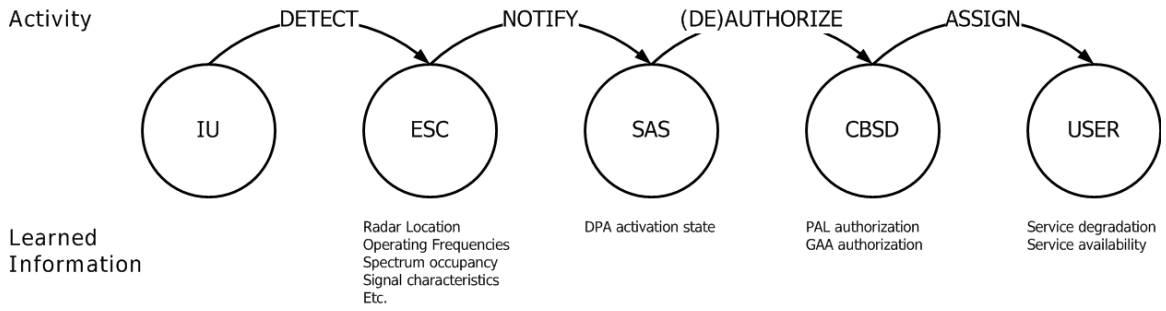

Illustration 3: Summary of learned information in IU protection process.

The Key Bridge architecture, design, implementation and operational strategy complies with the letter and spirit of all industry multi-stakeholder group and DoD / NTIA requirements, recommendations and requests of which we are aware. These include but are not limited to:

Wireless Innovation Forum published documents

- CBRS Requirements for Commercial Operation
- CBRS Communications Security Technical Specification
- CBRS Operational Security Technical Specification

DoD provided documents

- Requirements for 3550 MHz Environmental Sensing Capability Test and Certification [DRAFT]

NTIA provided documents

- Distinction Between Radar Declaration and Pulse Burst Detection in 3.5 GHz Spectrum Sharing Systems (TM-17-526) [DRAFT]

- Procedures for Laboratory Testing of Environmental Sensing Capability Sensor Devices (TM-17-527) [DRAFT]

_END